IN THE CLAIMS:

Amended claims follow:

1. (Currently Amended) A computer program product comprising a computer program operable to control a computer to detect a malicious alteration to a stored computer file, said computer program comprising:

file comparing logic operable to directly compare the entire contents of said stored computer file with the entire contents of an archive copy of said computer file as stored when said stored computer file was created; and

comparison response logic operable if said file comparing logic detects that the entire contents of said stored computer file and the entire contents of said archive computer file do not match to trigger further countermeasures against a potential malicious alteration;

wherein a subset of file types stored by said computer are subject to comparison by said file comparing logic and to creation of an archive copy for use with said file comparing logic;

wherein, upon creation of said stored computer file, said archive copy of said computer file is also created;

wherein said archive copy of said computer file is created for a subset of file types stored by said computer;

wherein said subset of file types includes one or more of:

executable file types; and

dynamic link library file types.

2. (Original) A computer program product as claimed in claim 1, wherein said further countermeasures include scanning said stored computer file using a library of computer virus definition data to identify a computer virus infection of said stored computer file.

3. (Original) A computer program product as claimed in claim 1, wherein said archive copy of said computer file is stored in one of:

an unencrypted form;

an encrypted form;

an encrypted media;

an encrypted volume; and

a PGP disk.

4. (Original) A computer program product as claimed in claim 1, wherein said archive copy of said computer file is stored in one of:

a different physical storage device to said stored computer file; and

a different part of a common physical storage device shared with stored computer file.

5. – 9. (Cancelled)

10. (Currently Amended) A method of detecting a malicious alteration to a stored computer file, said method comprising the steps of:

directly comparing the entire contents of said stored computer file with the entire contents of an archive copy of said computer file as stored when said stored computer file was created; and

if said file comparing step detects that the entire contents of said stored computer file and the entire contents of said archive computer file do not match, triggering further countermeasures against a potential malicious alteration;

wherein a subset of file types stored by said computer are subject to comparison by file comparing logic and to creation of an archive copy for use with said file comparing logic;

wherein, upon creation of said stored computer file, said archive copy of said computer file is also created;

wherein said archive copy of said computer file is created for a subset of file types stored by said computer;

wherein said subset of file types includes one or more of:

executable file types; and

dynamic link library file types.

11. (Original) A method as claimed in claim 10, wherein said further countermeasures include scanning said stored computer file using a library of computer virus definition data to identify a computer virus infection of said stored computer file.

12. (Original) A method as claimed in claim 10, wherein said archive copy of said computer file is stored in one of:

an unencrypted form;

an encrypted form;

an encrypted media;

an encrypted volume; and

a PGP disk.

13. (Original) A method as claimed in claim 10, wherein said archive copy of said computer file is stored in one of:

a different physical storage device to said stored computer file; and

a different part of a common physical storage device shared with stored computer file.

14. – 18. (Cancelled)

19. (Currently Amended) Apparatus for processing data operable to detect a malicious alteration to a stored computer file, said apparatus comprising:

a file comparator operable to directly compare the entire contents of said stored computer file with the entire contents of an archive copy of said computer file stored when said as stored computer file was created; and

a comparison responder operable if said file [comparing logic]comparator detects that the entire contents of said stored computer file and the entire contents of said

archive computer file do not match to trigger further countermeasures against a potential malicious alteration;

wherein a subset of file types stored by said computer are subject to comparison by said file comparator and to creation of an archive copy for use with said file comparator;

wherein, upon creation of said stored computer file, said archive copy of said computer file is also created;

wherein said archive copy of said computer file is created for a subset of file types stored by said computer;

wherein said subset of file types includes one or more of:

executable file types; and

dynamic link library file types.

20. (Original) Apparatus as claimed in claim 19, wherein said further countermeasures include scanning said stored computer file using a library of computer virus definition data to identify a computer virus infection of said stored computer file.

21. (Original) Apparatus as claimed in claim 19, wherein said archive copy of said computer file is stored in one of:

an unencrypted form;

an encrypted form;

an encrypted media;

an encrypted volume; and

a PGP disk.

22. (Original) Apparatus as claimed in claim 19, wherein said archive copy of said computer file is stored in one of:

a different physical storage device to said stored computer file; and

a different part of a common physical storage device shared with stored computer file.

23. – 27. (Cancelled)